AMENDMENTS TO THE CLAIMS

Claim 1 (currently amended): System for reading a document comprising a card provided with machine-readable holder details in a machine readable zone and for establishing whether a person presenting the document has a predetermined right, which document at least contains a chip containing one or more private keys and a biocertificate containing biometric data on the ~~biometric data on a~~ holder as well as data with a predetermined relationship to the machine readable holder details in the machine readable zone which predetermined relationship is based on a one-way function, and wherein the system comprises:

- a reader for reading the chip and for reading the machine-readable holder details in the machine readable zone;
- a memory containing details with regard to the predetermined right of the holder;
- a biometric feature scanner arranged to scan a biometric feature of the holder and to generate scanned biometric data;
- a processing unit that is connected to the reader, the memory and the biometric feature scanner and is equipped to:
  - establish the authenticity of the chip by transmitting a random challenge code to the chip, receiving a digitally signed random challenge code from the chip that is obtained by digitally signing said random challenge code by said chip using one of said one or more private keys and checking the digitally signed challenge code with a certificate from an issuing authority,
  - establish the authenticity of the ~~biometric~~ data in the biocertificate by receiving digitally signed biocertificate data that is obtained by digitally signing said data in said biocertificate by said chip using one of said one or more private keys and checking the digitally signed biocertificate data with the certificate from said issuing authority, and ~~of the data having the predetermined relationship to the machine readable holder details with the aid of a public key encryption technology;~~
  - ~~receive the biometric data on the holder from the chip, from the reader;~~

- receive the scanned biometric data on the person presenting the document from the biometric feature scanner and to compare these with the biometric data on the holder from the chip as present in said digitally signed biocertificate data to determine whether the person presenting the document is the holder;
- receive the machine readable holder details in the machine readable zone via the reader, check said one-way functional ~~the predetermined~~ relationship between the holder details and the data having said one-way functional ~~the predetermined~~ relationship to the machine readable holder details in order to authenticate the machine readable holder details in the machine readable zone; ~~and~~
- read the predetermined right of the holder from the memory; and
- provide a signal to indicate the predetermined right for the person presenting the document if the chip, the ~~biometric~~ biocertificate data and the machine readable holder details ~~data~~ are authentic, the predetermined relationship has been established and the person presenting the document is the same as the holder.

Claim 2 (original): System according to Claim 1, wherein the document is a travel document.

Claim 3 (cancelled)

Claim 4 (currently amended): System according to Claim 1[[3]], wherein the one-way function is a hashing function.

Claim 5 (currently amended): Method for reading a document comprising a card provided with machine-readable holder details in a machine readable zone and for establishing whether a person presenting the document has a predetermined right, which document contains at least one chip containing one or more private keys and a biocertificate containing biometric data on a holder as well as data with ~~having~~ a predetermined relationship to the machine readable holder details in the machine readable zone which predetermined relationship is based on a one-way function, and wherein the method ~~system~~ comprises ~~a reader for reading the chip and for reading the machine-readable holder details in the machine readable zone, a memory containing data on the predetermined right of the holder, a biometric feature scanner arranged to scan a biometric~~

~~feature of the holder and to generate scanned biometric data and a processing unit that is connected to the reader, the memory and the biometric feature scanner, wherein the method comprises the following operations performed by the processing unit~~:

- establishing authenticity of the chip by transmitting a random challenge code to the chip, receiving a digitally signed random challenge code from the chip that is obtained by digitally signing said random challenge code by said chip using one of said one or more private keys and checking the digitally signed challenge code with a certificate from an issuing authority;
- establishing the authenticity of the data in the biocertificate by receiving digitally signed biocertificate data that is obtained by digitally signing said data in said biocertificate by said chip using one of said one or more private keys and checking the digitally signed biocertificate data with the certificate from said issuing authority;
- ~~establishment of the authenticity of the chip, of the biometric data and of the data having the predetermined relationship to the machine readable holder details with the aid of a public key encryption technology;~~
- ~~receipt of the biometric data on the holder from the chip;~~
- ~~receipt of the~~ receiving scanned biometric data on the person presenting the document from a biometric feature scanner and to compare these ~~comparison~~ with the biometric data on the holder from the chip as present in said digitally signed biocertificate data to determine whether the person presenting the document is the holder;
- ~~receipt of~~ receiving the machine readable holder details in the machine readable zone via a reader, checking said one-way functional relationship between the holder details and the data having said one-way functional relationship to the machine readable holder details in order to authenticate the machine readable holder details in the machine readable zone ~~of the specific relationship between the holder details and the data having the predetermined relationship to the machine readable holder details and reading the predetermined right of the holder from the memory~~;
- reading the predetermined right of the holder from a memory; and

- ~~provision of~~ providing a signal to indicate the predetermined right for the person presenting the document if the chip, the biocertificate ~~biometric~~ data and the machine readable holder details ~~data~~ are authentic, the predetermined relationship has been established and the person presenting the document is the same as the holder.

Claim 6 (currently amended): Data carrier device comprising a computer program that can be loaded by a system for reading a document comprising a card provided with machine-readable holder details in a machine readable zone and for establishing whether a person presenting the document has a predetermined right, which document ~~contains~~ at least contains a ~~one~~ chip containing one or more private keys and a biocertificate containing biometric data on the ~~a~~ holder as well as data with ~~having~~ a predetermined relationship to the machine readable holder details in the machine readable zone which predetermined relationship is based on a one-way function, and ~~wherein the system comprises a reader for reading the chip and for reading the machine readable holder details in the machine readable zone, a memory containing data on the predetermined right of the holder, a biometric feature scanner arranged to scan a biometric feature of the holder and to generate scanned biometric data and a processing unit that is connected to the reader, the memory and the biometric feature scanner,~~ wherein the computer program can provide the system with the following functionality:

- ~~establishment of~~ establishing the authenticity of the chip by transmitting a random challenge code to the chip, receiving a digitally signed random challenge code from the chip that is obtained by digitally signing said random challenge code by said chip using one of said one or more private keys and checking the digitally signed challenge code with a certificate from an issuing authority~~, of the biometric data and of the data having the predetermined relationship to the machine readable holder details with the aid of a public key encryption technology~~;
- establishing the authenticity of the data in the biocertificate by receiving digitally signed biocertificate data that is obtained by digitally signing said data in said biocertificate by said chip using one or said one or more private keys and checking the digitally signed biocertificate data with the certificate from said issuing authority;

- ~~receipt of the biometric data on the holder from the chip;~~
- ~~receipt of the~~ receiving scanned biometric data on the person presenting the document from a biometric feature scanner and to compare these ~~comparison with~~ the biometric data on the holder from the chip as present in said digitally signed biocertificate data to determine whether the person presenting the document is the holder;
- ~~receipt of~~ receiving the machine readable holder details in the machine readable zone via a reader, checking said one-way functional relationship between the holder details and the data having said one-way functional relationship to the machine readable holder details in order to authenticate the machine readable holder details in the machine readable zone ~~of the specific relationship between the holder details and the data having the predetermined relationship to the machine readable holder details and reading the predetermined right of the holder from the memory~~;
- reading the predetermined right of the holder from a memory; and
- ~~provision of~~ providing a signal to indicate the predetermined right for the person presenting the document if the chip, the biocertificate data and the machine readable holder details ~~and the data~~ are authentic, the predetermined relationship has been established and the person presenting the document is the same as the holder.

Claim 7 (cancelled)

Claim 8 (currently amended): Document comprising a card provided with machine-readable holder details in a machine readable zone and for establishing whether a person presenting the document has a predetermined right and a chip, which chip is provided with a processing unit and memory connected thereto and an input/output unit, wherein the memory contains one or more private keys and a biocertificate containing biometric data on a holder, as well as data that have a predetermined relationship to the machine readable holder details in the machine readable zone which predetermined relationship is based on a one-way function, as well as instructions for making the processing unit carry out the following operations:

- communication with a system according to Claim 1 to enable the authenticity of the chip and of said data in said biocertificate to be established with the aid of a public key encryption technology by performing the following operations:[[;]]
- ~~transmission of the biometric data on the holder and the data having the predetermined relationship to the machine readable holder details from the memory to the system.~~
  - receiving a random challenge code, digitally signing said random challenge code using one of said one or more private keys rendering a digitally signed random challenge code and transmitting said digitally signed random challenge code via said input/output unit to said system,
  - digitally signing said data in the biocertificate using one of said one or more private keys rendering digitally signed biocertificate data and transmitting said digitally signed biocertificate data via said input/output unit to said system.

Claim 9 (previously presented): Document according to Claim 8, wherein the document is a travel document.

Claim 10 (previously presented): Document according to Claim 9, wherein the chip is an integral part of the travel document.

Claim 11 (previously presented): Document according to Claim 8, wherein the input/output unit is equipped for contact-free communication.

Claim 12 (previously presented): Document according to Claim 8, wherein the chip is equipped as a transponder unit.

Claim 13-25 (cancelled)